



Reviewer's Guide

To AdRem NetCrunch

Table of Contents

ABOUT NETCRUNCH..... 3
PRICING AND LICENSING 3
NETCRUNCH EDITIONS 3
FUNCTIONAL OVERVIEW 4
SYSTEM REQUIREMENTS 6
ABOUT ADREM SOFTWARE 7

About NetCrunch

| | |
|---|---|
| Product name | AdRem NetCrunch |
| Current version | 6.5 released in November, 2010 |
| First released | 2002 |
| 30-day evaluation version download | http://www.adremsoft.com/demo |
| List of upgrades in the current version | http://www.adremsoft.com/netcrunch/page/whats-new |

Pricing and Licensing

AdRem NetCrunch is licensed per number of monitored nodes. It does not limit the number of network services, performance counters, or interfaces that you can monitor on these nodes.

NetCrunch comes in two editions, **Premium** and **Premium XE**, the later includes several mechanisms that optimize agentless monitoring in network environments larger than a few hundred nodes. Pricing starts at **USD 2 595** for monitoring up to 125 nodes.

NetCrunch Editions

NetCrunch comes in two editions: Premium and Premium XE. NetCrunch Premium is recommended for small networks with a couple of hundred nodes. NetCrunch Premium XE meets the increasing demand for an enterprise network monitoring.

NetCrunch available Node Licensing Packages:

- Premium 125
- Premium 300
- Premium XE 600
- Premium XE 1000
- Premium XE Unlimited

Read more about NetCrunch editions at: <http://www.adremsoft.com/netcrunch/page/editions>

NetCrunch Remote Access Licensing:

NetCrunch offers an option of remote access for several connections. Dependant on the license type 1, 5, 10 or unlimited number of users can have remote access at one time. Not all Node Licensing Packages and **Remote Access** options combinations are available.

Read more about NetCrunch licensing at: <http://www.adremsoft.com/netcrunch/page/licensing>

Functional Overview

NetCrunch in a Nutshell

NetCrunch 6 is a comprehensive network management and application monitoring solution for networks of up to several thousand nodes.

NetCrunch unifies fault management by collecting and alerting on events received from a variety of external sources such as: Windows Event Logs, Syslog, SNMP traps.

NetCrunch consists of WMI, SSH and SNMP monitors for monitoring of diverse operating systems and networking devices. It contains over 65 built-in Network Service monitors and 5 advanced user experience monitors (HTTP/S, POP3, FTP, SMTP, DNS).

Auto Discovery

NetCrunch automatically (and periodically) discovers TCP/IP nodes in order to create an accurate view of the network and to draw maps of logical and physical topologies. To make the network discovery process complete, the program is shipped with predefined filtered views and pre-configured Monitoring Polices. Discovered devices are automatically classified and added to relevant views. After completing the network scan, NetCrunch determines network relations between nodes and intermediate routers to set up monitoring dependencies for each node. Besides finding nodes, the program also detects network services they are providing.

Event Management

NetCrunch processes events coming from a variety of sources. Some of them may be external like *SNMP Traps* or *Windows Event Log* entries and others generated by NetCrunch like *Monitoring Events* (node state changed) or *Atlas Events* (like new node discovered).

Actions assigned to an event can be performed immediately or after some time if the event has not been cleared. Most of the built-in events are correlated and when the event condition changes they are automatically cleared.

Availability Monitoring

Some services (or devices) can be checked by a simple PING where some others can be checked more thoroughly by Network Services monitors. We call these monitors *intelligent* because they can check not only connectivity but also response received.

Monitoring of key services can be performed on multiple levels. As the low level checks only basic service answer (it's usually some kind of HELLO), the higher levels of monitoring allow to check for more specific things like authentication (HTTP, FTP, POP3, SMTP, DNS) or if the service is operating properly (i.e. downloading file, receiving and sending test email).

Network Performance Monitoring

NetCrunch allows agentless performance monitoring of different network devices (SNMP), operating systems, and applications running on top of Windows or UNIX/Linux. This is realized by monitoring selected performance counters values and triggering alerts. All those values can be collected and stored for later long term trend analysis.

Program enables agentless monitoring of servers (Windows, Linux, Mac OS X, BSD, and NetWare) from a unified interface. NetCrunch requires administrator credentials to connect to servers and gather statistics about performance counters.

Monitoring Policies

Monitoring policies are sets of rules defining events which need to be monitored and which data that should be collected for later reporting. One node can be assigned to multiple policies; it can also have its own policy defined that may override map or atlas policy definitions.

Trend Viewer

Data collected by NetCrunch can be used for reporting or for on demand trend analysis. Performance history of a single counter can be compared across multiple nodes on a single chart to determine under- and over-utilized resources.

The program automatically initiates data collection, based on monitoring policies to generate reports. Reports are also generated on demand or periodically delivered by e-mail to selected recipients.

Users can export the data collected by NetCrunch to an industry standard databases for further analysis and to diagnose with external reporting tools.

Remote Access

Administrators can access NetCrunch remotely using NetCrunch Administration Console or the web-based client.

NetCrunch allows creating profiles for remote users (available only with web connection), limiting their access to certain network maps or program functions. All remote access sessions can be logged by NetCrunch, showing which users connected remotely to NetCrunch, from what IP address and what tasks they performed. Fast and secure communication with NetCrunch is possible thanks to the encryption and compression algorithm.

NetCrunch Connection Broker allows receiving desktop notifications from multiple NetCrunch Servers. The programs also allow viewing events details, and manage credentials needed to connect to different NetCrunch Servers via *NetCrunch Administration Console*.

System Requirements

| | NETCRUNCH CONSOLE | NETCRUNCH SERVER |
|-------------------------|--|--|
| Processor | Intel Core Solo 1.33 GHz | Intel Core 2 Duo |
| RAM Memory | 1 GB | 2 GB |
| Free Disk Space | 2 GB | 4 GB |
| Display | 1280x1024 True Color | 1024x768 True Color |
| Web Browser | - | Internet Explorer 7 or later, Firefox 3 |
| Operating System | Windows 7/Vista SP2/XP SP3 or Windows 2003/2008 (x32/x64) | Windows Server 2008/2003 x32 (x32/x64 editions) |

Detailed System Recommendations for NetCrunch 6.x:

<http://www.adremsoft.com/netcrunch/page/system-recommendation>

The recommended system requirements should be applied for monitoring of more than 500 nodes by NetCrunch network monitoring software.

For VMware installation read our VMware Support Statement:

<http://www.adremsoft.com/netcrunch/features/vmware-support-statement>

About AdRem Software

AdRem Software is a company with over 11 years of experience in IT industry. It provides network management solutions for businesses that seek affordable ways to maximize ROI on IT infrastructures. AdRem's solutions are sold through company's resellers, distributors and system integrators and deployed on servers in over 70 countries on all continents.

Company Address

AdRem Software, Inc.
410 Park Avenue, 15th Floor
New York, NY 10022
Phone: +1 (212) 319-4114
Fax: +1 (212) 832-4114
<http://www.adremsoft.com>

E-mail for customer contact:

sales@adremsoft.com

Press Room

www.adremsoft.com/pressroom

Press Releases

<http://www.adremsoft.com/pressroom/releases>

Public Relations Contact

Marek Tyniec
Phone: +1 (212) 319-4114
Fax: +1 (212) 832-4114
pr@adremsoft.com